JOURNAL OF NUMBER THEORY 40, 359–375 (1992)

The Genus Field of an Algebraic Function Field

ROSARIO CLEMENT

Departamento de Matemáticas, Universidad del Pais Vasco, Apartado de Correos 644, 48080 Bilbao, Vizcaya, Spain

Communicated by D. Goss

Received October 3, 1990; revised February 11, 1991

INTRODUCTION

In this paper our purpose is to present an analogue to the theory of the genus field of an algebraic number field into the algebraic function fields context, somehow inspired by papers of Goss, Rosen, and Hayes, and taking as a starting point, the exposition given by Hasse [6] of the genus field of a quadratic number field.

Let $k=\mathbb{F}_q(T)$ be the field of rational functions over the finite field $\mathbb{F}_q$, l a prime dividing $q-1$, and K a cyclic extension of k of degree l, so that $K=k(\sqrt[l]{P(T)})$ with $P(T)$ a polynomial of $\mathbb{F}_q[T]$; let θ_K be the integral closure of $\mathbb{F}_q[T]$ in K, and ∞—that we call the infinite prime of k—the prime divisor of k corresponding to the prime ideal of the subring $\mathbb{F}_q[1/T]$ of k generated by $1/T$.

In the classical context in which F is a quadratic number field, the genus field of F is the maximal abelian extension of $\mathbb{Q}$ contained in the Hilbert class field of F. The notion of Hilbert class field has no proper analogue for algebraic function fields; there are however several "partial" analogues (see [8], [12]), depending on which features one focuses attention on. Now, the Hilbert class field of a quadratic number field F is the finite abelian extension of F such that the prime ideals of the ring of integers θ_F of F splitting there are precisely the principal ideals generated by an element of positive norm, that is, whose norm is a square in $\mathbb{R}$. In our context we look for a finite abelian extension of K, denoted by $H^{(+)}$, such that the prime ideals of θ_K splitting in it, are precisely the principal ideals generated by an element whose norm (with respect to k) is an l-power in k_∞, the completion of k with respect to ∞. In Section 1 we prove the existence of such an extension $H^{(+)}$. In Sections 2 and 3 we describe explicitly the greatest abelian extension Γ of k contained in $H^{(+)}$, and we compute the number of "ambiguous classes"; the results exhibited in both sections show a great similarity with the classical results for quadratic fields, and we call Γ the

0022-314X/92 $3.00

genus field of K with respect to k. Finally in Section 4, making use of the reciprocity law, we give a characterization of the prime ideals of θ_K which split in Γ.

1

We call infinite primes of K the prime divisors $\infty_1, ..., \infty_i$ whose restriction to k is the prime divisor ∞—of course $i=1$ if ∞ ramifies or remains inert in K, and $i=l$ otherwiwse, that is, if ∞ splits completely in K—k_∞ and K_{∞_j} will denote respectively the completions of k and K for the prime divisors ∞ and ∞_j, and we put

$$\Delta = \left\{ (\alpha_1, ..., \alpha_i) \in \prod_{j=1}^{i} K_{\infty_j} \mid N_{K_{\infty_1} \times \cdots \times K_{\infty_i}/k_\infty}(\alpha_1, ..., \alpha_i) \in k_\infty^{*l} \right\},$$

where $N_{K_{\infty_1} \times \cdots \times K_{\infty_i}/k_\infty} : K_{\infty_1} \times \cdots \times K_{\infty_i} \to k_\infty$ denotes the norm map.

PROPOSITION 1.1. *If $U_\mathfrak{p}$ denotes the unit group of the completion $K_\mathfrak{p}$ of K at a prime ideal $\mathfrak{p}$ of θ_K, the index of $K^*(\Delta \times \prod_{\mathfrak{p} \in \operatorname{Max} \theta_K} U_\mathfrak{p})$ in the idèle group J_K of K is finite.*

Proof. We have

$$K^* \left(\Delta \times \prod_{\mathfrak{p} \in \operatorname{Max} \theta_K} U_\mathfrak{p} \right) \subseteq K^* \left(\prod_{j=1}^{i} K_{\infty_j}^* \times \prod_{\mathfrak{p} \in \operatorname{Max} \theta_K} U_\mathfrak{p} \right) \subseteq J_K.$$

On the one hand $J_K/K^*(\prod_{j=1}^{i} K_{\infty_j}^* \times \prod_\mathfrak{p} U_\mathfrak{p}) \simeq \operatorname{Pic} \theta_K$, the ideal class group of θ_K which is, of course, finite. (See [3], [10]).

On the other hand, we have

$$\begin{aligned}
&\left(K^* \left(\prod_{j=1}^{i} K_{\infty_j}^* \times \prod_{\mathfrak{p}} U_\mathfrak{p} \right) : K^* \left(\Delta \times \prod_{\mathfrak{p}} U_\mathfrak{p} \right) \right) \\
&\quad = \frac{(\prod_{j=1}^{i} K_{\infty_j}^* : \Delta)}{(K^* \cap (\prod_{j=1}^{i} K_{\infty_j}^* \times \prod_\mathfrak{p} U_\mathfrak{p}) : K^* \cap (\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}))} \\
&\quad = \frac{(\prod_{j=1}^{i} K_{\infty_j}^* : \Delta)}{(U_K : U_K^{(+)})},
\end{aligned}$$

where U_K denotes the unit group of θ_K and

$$U_K^{(+)} = \{\alpha \in U_K \mid N_{K/k}(\alpha) \in k_\infty^{*l}\}.$$

Since $(k_\infty^* : k_\infty^{*l}) = l^2$, from the homomorphism $\prod_{j=1}^{i} K_{\infty_j}^* \to k_\infty^*/k_\infty^{*l}$ induced by the norm, we obtain $(\prod_{j=1}^{i} K_{\infty_j}^* : \Delta) \mid l^2$; considering now the norm $N_{K/k}: K \to k$, we have

$$U_K/U_K^{(+)} \simeq N_{K/k}(U_K)/F_q^{*l} \subset \mathbb{F}_q^*/\mathbb{F}_q^{*l}$$

so that $(U_K : U_K^{(+)}) \mid l$, and the proposition follows. ∎

Remark. If ∞ ramifies or remains inert in K, $(J_K : K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})) = l . |\operatorname{Pic} \theta_K|$; otherwise, that is, if ∞ splits in K, $(J_K : K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})) = (l^2/(U_K : U_K^{(+)})) . |\operatorname{Pic} \theta_K|$.

Since $K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})$ is an open subgroup of J_K of finite index, that is, an admissible subgroup of J_K, we can define $H^{(+)}$ to be the class field of K corresponding to this subgroup of J_K. Consequently $H^{(+)}$ is the finite abelian extension of K, characterized by $\operatorname{Gal}(H^{(+)}/K) \simeq J_K/K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})$. Of course, $H^{(+)}/K$ is unramified at every prime ideal of θ_K.

PROPOSITION 1.2. *Let $\mathfrak{p}_0$ be a prime ideal of θ_K. Then $\mathfrak{p}_0$ splits completely in $H^{(+)}$ if and only if it is a principal ideal (β) with $N_{K/k}(\beta) \in k_\infty^{*l}$.*

Proof. $\mathfrak{p}_0$ splits completely in $H^{(+)}$ if and only if $K_{\mathfrak{p}_0}^* \subseteq K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})$. Let π_0 be a uniformizer of $K_{\mathfrak{p}_0}$; since $U_{\mathfrak{p}_0} \subseteq K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})$ it follows that

$$K_{\mathfrak{p}_0}^* \subseteq K^*\left(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}\right) \Leftrightarrow (1, 1, ..., \pi_0, 1, ...) \in K^*\left(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}\right) \Leftrightarrow \exists \beta \in K^*$$

such that

$$(\beta^{-1}, \beta^{-1}, ..., \beta^{-1}\pi_0, \beta^{-1}, ...) \in \Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}.$$

Now $K_{\infty_1} \times \cdots \times K_{\infty_i} \simeq k_\infty \otimes_k K$, thus

$$N_{K/k}(\alpha) = N_{K \otimes_k k_\infty/k_\infty}(\alpha \otimes 1) = N_{K_{\infty_1} \times \cdots \times K_{\infty_i}/k_\infty}(\alpha, ..., \alpha) \qquad \forall \alpha \in K$$

consequently

$$(\beta^{-1}, \beta^{-1}, ..., \beta^{-1}\pi_0, \beta^{-1}, ...) \in \Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}} \Leftrightarrow \begin{cases} \mathfrak{p}_0 = (\beta) \\ N_{K/k}(\beta) \in k_\infty^{*l} \end{cases}$$

which proves our assertion. ∎

COROLLARY 1.3. *If $(Q(T))$ is a prime ideal in $\mathbb{F}_q[T]$ which remains inert in K, the ideal $\mathfrak{p} = \theta_K(Q(T))$ splits completely in $H^{(+)}$.* ∎

PROPOSITION 1.4. *$H^{(+)}$ is a Galois extension of k.*

Proof. It follows at once from the fact that $\sigma(\Delta)=\Delta$ for any k-embedding σ of $H^{(+)}$ in the algebraic closure $\bar{k}$ of k. ▌

It will be useful later to handle the description of $\mathrm{Gal}(H^{(+)}/K)$ as a quotient group of the group of non-zero fractional ideals of θ_K. We shall write any idèle of J_K in the form $(a_\infty, (a_\mathfrak{p})_\mathfrak{p})$, where a_∞ denotes its "infinite component," that is, $a_\infty \in \prod_{j=1}^{i} K^*_{\infty_j}$, and $(a_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K^*_\mathfrak{p}$. We shall denote $J_K^{(+)}$ the subgroup of J_K, consisting of the idèles whose "infinite component" belongs to Δ, and

$$K^{(+)} = \{\alpha \in K^* \mid N_{K/k}(\alpha) \in k^{*i}_\infty\} = K^* \cap J_K^{(+)}.$$

LEMMA 1.5.

$$\frac{J_K^{(+)}}{K^{(+)}(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p})} \simeq \frac{J_K}{K^*(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p})}.$$

Proof. As a consequence of the approximation theorem for valuations, the canonical map $J_K^{(+)}/K^{(+)} \to J_K/K^*$ is surjective, hence an isomorphism. The image of $K^*(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p})/K^* \subset J_K/K^*$ through the above isomorphism, is the subgroup $(J_K^{(+)} \cap K^*(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}))/K^{(+)}$ of $J_K^{(+)}/K^{(+)}$. Now, clearly $\Delta \times \prod_\mathfrak{p} U_\mathfrak{p} \subseteq J_K^{(+)}$, consequently

$$J_K^{(+)} \cap K^*\left(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}\right) = K^{(+)}\left(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}\right)$$

and our assertion follows. ▌

PROPOSITION 1.6. *Let I_K denote the group of non-zero fractional ideals of θ_K and $P_K^{(+)}$ the subgroup of the principal fractional ideals (β) such that $\beta \in K^{(+)}$. Then*

$$\frac{J_K}{K^*(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p})} \simeq \frac{I_K}{P_K^{(+)}}.$$

Proof. The map $J_K^{(+)} \to I_K$ given by $(a_\infty, (a_\mathfrak{p})_\mathfrak{p}) \mapsto \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$ is surjective and its kernel is $\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}$; it follows that the sequence

$$1 \to K^{(+)}\left(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p}\right) \to J_K^{(+)} \to \frac{I_K}{P_K^{(+)}} \to 1$$

is exact; therefore

$$\frac{J_K^{(+)}}{K^{(+)}(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p})} \simeq \frac{I_K}{P_K^{(+)}}.$$

The proposition follows now from Lemma 1.5. ▌

In the following we write $\mathrm{Cl}\,\theta_K = I_K/P_K^{(+)}$, so that we have then the "reciprocity isomorphism"

$$\mathrm{Cl}\,\theta_K \simeq \mathrm{Gal}(H^{(+)}/K)$$

given by the Artin symbol $[\mathfrak{a}] \to ([\mathfrak{a}], H^{(+)}/K)$ for $[\mathfrak{a}] \in \mathrm{Cl}\,\theta_K$.

2

If, as previously, $K = k(\sqrt[l]{P(T)})$, we write $P(T) = aP_1(T)^{i_1} \cdots P_s(T)^{i_s}$ where $P_i(T)$ are monic irreducible polynomials. We prove in this section the following

THEOREM 2.1. *The greatest abelian extension of k contained in $H^{(+)}$ is*

$$\Gamma = \mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)}).$$

LEMMA 2.2. *Let F/E be a finite extension of function fields of one variable with finite constant field. Let H be an admissible subgroup of the idèle group J_F and F_H its class field; if E_0 is the greatest abelian extension of E contained in F_H, the corresponding subgroup of J_E is $E^* N_{F/E}(H)$.*

Proof. The proof of this well known result [4] is based on the main properties of the reciprocity map. The norm map $N_{F/E}\colon J_F \to J_E$ is open, hence $E^* N_{F/E}(H)$ is an open subgroup of J_E. On the other hand, from the fact that H/F^* is a subgroup of C_F of finite index (C_F denotes as usually the idèle class group of F, that is, $C_F = J_F/F^*$) it follows that $E^* N_{F/E}(H)/E^*$ is a subgroup of finite index of $N_{F/E}(C_F)$. Since F/E is a finite extension, $N_{F/E}(C_F)$ is also a subgroup of finite index of C_E, therefore $E^* N_{F/E}(H)$ is an admissible subgroup of J_E. In order to prove that its class field is precisely E_0, it is enough to show that such a subgroup is contained in the subgroup of J_E corresponding to any abelian extension E' of E contained in F_H. If H' denotes the admissible subgroup of J_F corresponding to the abelian extension FE'/F, we have $E^* N_{F/E}(H) \subseteq E^* N_{F/E}(H')$; now the diagram

$$\begin{array}{ccc} J_F & \longrightarrow & \mathrm{Gal}(FE'/F) \\ {\scriptstyle N_{F/E}}\downarrow & & \downarrow \\ J_E & \longrightarrow & \mathrm{Gal}(E'/E) \end{array}$$

is conmutative, therefore $E^* N_{F/E}(H)$ is contained in the subgroup of J_E corresponding to E'. ∎

According to the above lemma, if Γ denotes the greatest abelian extension of k contained in $H^{(+)}$, the subgroup of J_k corresponding to Γ is $k^*N_{K/k}(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}})$. Our next task is to compute $[\Gamma : k] = (J_k : k^*N_{K/k}(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}))$; for this purpose we must look first at the behaviour of the primes in the extension K/k.

PROPOSITION 2.3. *The prime ideals of* $\mathbb{F}_q[T]$ *which ramify in* K *are the* $(P_i(T))$ *for* $i = 1, ..., s$. *The infinite prime* ∞ *of* k *ramifies in* K *if and only if* $l \nmid \deg P(T)$; *it splits completely in* K/k *if and only if* $l \mid \deg P(T)$ *and* $a \in \mathbb{F}_q^{*l}$.

Proof. It is straightforward to check that the prime ideals $\{(P_i(T))\}_{i=1,...,s}$ of $\mathbb{F}_q[T]$ ramify in K/k. On the other hand, since l is a unity in $\mathbb{F}_q[T]$, if $\mathrm{Diff}(\theta_K/\mathbb{F}_q[T])$ denotes the Different of θ_K relative to $\mathbb{F}_q[T]$, we have

$$\mathrm{Diff}(\theta_K/\mathbb{F}_q[T]) \supseteq \theta_K(\sqrt[l]{P(T)})^{l-1}.$$

If $Q(T) \in \mathbb{F}_q[T]$ is an irreducible polynomial not dividing $P(T)$ and $\mathfrak{q}$ is a prime ideal of θ_K lying over $(Q(T))$, it is clear that $\mathfrak{q} \not\supset \mathrm{Diff}(\theta_K/\mathbb{F}_q[T])$, hence $(Q(T))$ doesn't ramify in K/k.

Next we recall that k_∞ denotes the completion of k at the infinite prime, so that $k_\infty = \mathbb{F}_q((1/T))$; if v_{∞_j} denotes the normalized valuation of K corresponding to the infinite prime ∞_j, we have

$$\begin{aligned} v_{\infty_j}(P(T)) &= l . v_{\infty_j}(\sqrt[l]{P(T)}) \\ &= -e_\infty . \deg P(T), \end{aligned}$$

where e_∞ is the ramification degree of ∞ in K/k.

If $l \nmid \deg P(T)$, $l \mid e_\infty$ hence $e_\infty = l$.

If $l \mid \deg P(T)$, we have

$$\begin{aligned} k_\infty(\sqrt[l]{P(T)}) &= k_\infty(\sqrt[l]{aT^d + \cdots + a_d}) \\ &= k_\infty(\sqrt[l]{a + a_1(1/T) + \cdots + a_d(1/T)^d}); \end{aligned}$$

$a + a_1(1/T) + \cdots + a_d(1/T)^d$ is a unity in k_∞ and $(l, q) = 1$, therefore the extension $k_\infty(\sqrt[l]{P(T)})/k_\infty$ is unramified, thus ∞ doesn't ramify in K/k. On the other hand,

$$\begin{aligned} \infty \text{ splits completely in } K/k &\Leftrightarrow [k_\infty(\sqrt[l]{P(T)}) : k_\infty] = 1 \\ &\Leftrightarrow a + a_1 T + \cdots + a_d(1/T)^d \in k_\infty^{*l} \\ &\Leftrightarrow a \in \mathbb{F}_q^{*l} \qquad \text{(by Hensel's lemma).} \quad \blacksquare \end{aligned}$$

PROPOSITION 2.4. *With the above notations* $[\Gamma : k] = l^{s+1}$.

Proof. For any irreducible polynomial $Q(T) \in \mathbb{F}_q[T]$, recalling that $U_{(Q)}$ denotes the unit group of the completion $k_{(Q)}$ of k with respect to the prime ideal $(Q(T))$, we write $U_{(Q)}^{(1)} = \{x \in U_{(Q)} \mid v_Q(x-1) \geqslant 1\}$ where v_Q is the discrete valuation of $k_{(Q)}$. Since we know that the only prime ideals of $\mathbb{F}_q[T]$ which ramify in K/k are $\{(P_i(T))\}_{i=1,\dots,s}$ and that they do it totally and tamely, according to well-known properties of the norm map in local fields extensions (see [2] or [13]) we have

$$\begin{aligned} &k^* N_{K/k}\left(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}\right) \\ &\quad = k^* \left(k_\infty^{*l} \times U_{(P_1)}^{(1)} \mathbb{F}_{q^{\deg P_1}}^{*l} \times \cdots \times U_{(P_s)}^{(1)} \mathbb{F}_{q^{\deg P_s}}^{*l} \times \prod_{(Q) \neq (P_i)} U_{(Q)}\right). \end{aligned}$$

Moreover $J_k = k^*(k_\infty^* \times \prod_{(Q)} U_{(Q)})$, hence

$$\begin{aligned} \left(J_k : k^* N_{K/k}\left(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}\right)\right) = \Bigg(\Bigg(k_\infty^* \times \prod_{(Q)} U_{(Q)}\Bigg) &: \Bigg(k_\infty^{*l} \times U_{(P_1)}^{(1)} \mathbb{F}_{q^{\deg P_1}}^{*l} \\ &\times \cdots \times U_{(P_s)}^{(1)} \mathbb{F}_{q^{\deg P_s}}^{*l} \times \prod_{(Q) \neq (P_i)} U_{(Q)}\Bigg)\Bigg) \Big/ (\mathbb{F}_q^* : \mathbb{F}_q^{*l}). \end{aligned}$$

Here $(\mathbb{F}_q^* : \mathbb{F}_q^{*l}) = l$ and $(k_\infty^* : k_\infty^{*l}) = l^2$; besides $U_{(P_i)} \simeq U_{(P_i)}^{(1)} \times (\mathbb{F}_q[T]/(P_i(T)))^*$ yields $(U_{(P_i)} : U_{(P_i)}^{(1)} \mathbb{F}_{q^{\deg P_i}}^{*l}) = l$, for all $i = 1, \dots, s$. Therefore the above index—which is equal to $[\Gamma : k]$—is $l^2 l^s / l$. ∎

PROPOSITION 2.5. *Every extension of K which is unramified in the prime ideals of* θ_K *and a composition of cyclic extensions of k of degree l is contained in* $H^{(+)}$.

Proof. We contend that $K^*(\Delta \times \prod_{\mathfrak{p}} U_{\mathfrak{p}}) \subseteq K^* N_{K'/K}(J_{K'})$ for any extension K'/K which is unramified in the finite primes of K and a composition of cyclic extensions of k of degree l; that will prove the proposition, by class field theory.

The properties of the reciprocity map give the commutativity of the diagram

$$\begin{tikzcd} \Delta \arrow[r] & J_K \arrow[r, "\text{rec.}"] \arrow[d, "N_{K/k}"] & \mathrm{Gal}(K'/K) \arrow[d] & \\ & J_k \arrow[r, "\text{rec.}"] & \mathrm{Gal}(K'/k) \arrow[r, "\sim"] & \mathbb{Z}/l\mathbb{Z} \times \cdots \times \mathbb{Z}/l\mathbb{Z}; \end{tikzcd}$$

according to the definition of Δ, the norm of any $\alpha \in \Delta \subseteq J_K$, is an idèle of J_k of the form $(\beta, 1, 1, \ldots)$ with $\beta \in k_\infty^{*l}$; clearly $(\beta, 1, 1, \ldots) \in J_k^l$ and therefore belongs to the kernel of the reciprocity map $J_k \to \mathrm{Gal}(K'/k) \simeq \mathbb{Z}/(l) \times \cdots \times \mathbb{Z}/(l)$. Hence the image of Δ in J_K is contained in the kernel of the map $J_K \to \mathrm{Gal}(K'/K)$, that is, $\Delta \subseteq K^* N_{K'/K}(J_{K'})$.

Now, since K'/K is unramified, $U_\mathfrak{p} \subseteq N_{K'/K}(J_{K'})$ for any prime ideal $\mathfrak{p}$ of θ_K; consequently

$$K^* \left(\Delta \times \prod_\mathfrak{p} U_\mathfrak{p} \right) \subseteq K^* N_{K'/K}(J_{K'}). \quad \blacksquare$$

Proof of Theorem 2.1. Let us check first that $\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)})/K$ is unramified: Let $\mathfrak{q}$ be a prime ideal of θ_K and $(Q(T)) = \mathfrak{q} \cap \mathbb{F}_q[T]$; if $(Q(T))$ ramifies in $\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)})/K$ necessarily $(Q(T)) = (P_i(T))$ for some i; furthermore

$$e_{\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)})/k}(P_i(T)) = e_{k(\sqrt[l]{P_i(T)})/k}(P_i(T)) = l;$$

since $e_{K/k}(P_i(T)) = l$, it follows that $\mathfrak{q}$ doesn't ramify in $\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)})$.

On the other hand $\mathrm{Gal}(\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)})/k) \simeq \mathbb{Z}/(l) \times \cdots \times \mathbb{Z}/(l)$, therefore, by Proposition 2.5, $\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)}) \subseteq H^{(+)}$, hence

$$\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)}) \subseteq \Gamma.$$

Since $[\Gamma : k] = l^{s+1} = [\mathbb{F}_{q^l}(T, \sqrt[l]{P_1(T)}, \ldots, \sqrt[l]{P_s(T)}) : k]$, the theorem is proved. $\blacksquare$

Because of the considerable analogy between the results obtained both in this section and the following one, on the one hand, and the well-known genus theory of quadratic fields on the other, we call Γ the genus field of K with respect to k.

3

With the notations introduced in the previous sections and writing $\mathrm{Gal}(K/k) = G$, our aim is to determine the number of "ambiguous" classes in $\mathrm{Cl}\, \theta_K$, that is, the order of the group $(\mathrm{Cl}\, \theta_K)^G$ consisting of all the ideal classes of $\mathrm{Cl}\, \theta_K$ left invariant under the natural action of G. (See [11]).

Both $K^{(+)}$ and $U_K^{(+)}$ are G-modules under the natural action of G; in the next propositions, we compute the orders of the cohomology groups $H^1(G, K^{(+)})$ and $H^1(G, U_K^{(+)})$.

PROPOSITION 3.1. *$H^1(G, K^{(+)})$ is a group of order $l^2/e_\infty f_\infty$ where e_∞ and f_∞ denote, as usually, the ramification and residual degree of ∞ in K/k, respectively.*

Proof. By Hilbert's Theorem 90 the cohomology sequence associated to the exact sequence

$$1 \to K^{(+)} \to K^* \to K^*/K^{(+)} \to 1$$

is

$$1 \to k^* \to k^* \to (K^*/K^{(+)})^G \to H^1(G, K^{(+)}) \to 1;$$

therefore $H^1(G, K^{(+)}) \simeq (K^*/K^{(+)})^G$. Clearly $\sigma(\alpha)/\alpha \in K^{(+)}$, $\forall \alpha \in K^*$, and $\forall \sigma \in G$, hence $(K^*/K^{(+)})^G = K^*/K^{(+)}$. On the other hand the canonical map

$$K^* \to \prod_{j=1}^{i} K^*_{\infty_j} \to \prod_{j=1}^{i} K^*_{\infty_j}/\Delta$$

gives the isomorphism

$$K^*/K^{(+)} \simeq \prod_{j=1}^{i} K^*_{\infty_j}/\Delta$$

(surjectivity is ensured by the approximation theorem for valuations). It remains to compute the order of $\prod_{j=1}^{i} K^*_{\infty_j}/\Delta$; this follows from the exact sequence

$$1 \longrightarrow \frac{\prod_{j=1}^{i} K^*_{\infty_j}}{\Delta} \xrightarrow{\mathcal{N}} \frac{k^*_\infty}{k^{*l}_\infty} \longrightarrow \frac{k^*_\infty}{N_{\prod_{j=1}^{i} K_{\infty_j}/k_\infty}(\prod_{j=1}^{i} K^*_{\infty_j})} \longrightarrow 1,$$

where $\mathcal{N}$ is induced by the norm—taking into account that $(k^*_\infty : k^{*l}_\infty) = l^2$ and that (by local class field theory)

$$\left(k^*_\infty : N_{\prod_{j=1}^{i} K_{\infty_j}/k_\infty}\left(\prod_{j=1}^{i} K^*_{\infty_j}\right)\right) = e_\infty f_\infty. \quad \blacksquare$$

PROPOSITION 3.2. *$H^1(G, U_K^{(+)})$ is a group of order $l^2/e_\infty f_\infty$.*

Proof. Since $U_K/U_K^{(+)}$ is a finite group (in fact $(U_K : U_K^{(+)}) = 1$ or l), the Herbrand quotient $h(G, U_K/U_K^{(+)})$ is equal to 1, thus $h(G, U_K^{(+)}) = h(G, U_K)$; but the Herbrand quotient $h(G, U_K)$ is well known (see, for instance, Artin and Tate [1]): $h(G, U_K) = e_\infty f_\infty/l$. Therefore, in order to prove our assertion it will suffice to compute the order of $H^2(G, U_K^{(+)})$. Now, considering the Tate cohomology groups we have

$$\hat{H}_0(G, U_K^{(+)}) = (U_K^{(+)})^G / N_{K/k}(U_K^{(+)}) = \mathbb{F}_q^*/\mathbb{F}_q^{*l};$$

hence, since G is cyclic,

$$|H^2(G, U_K^{(+)})| = |\hat{H}^2(G, U_K^{(+)})| = |\hat{H}^0(G, U_K^{(+)})| = l,$$

and the result follows. ∎

THEOREM 3.3. *If* $\mathrm{Cl}\,\theta_K = I_K/P_K^{(+)}$ *denotes the ideal classes group of* θ_K *corresponding to the class field* $H^{(+)}$ *of* K *and* $G = \mathrm{Gal}(K/k)$, *the order of* $(\mathrm{Cl}\,\theta_K)^G$ *is* l^s.

Proof. It is a well-known fact that $H^1(G, I_K) = \{1\}$; hence, the exact cohomology sequence attached to the exact sequence

$$1 \to P_K^{(+)} \to I_K \to \mathrm{Cl}\,\theta_K \to 1$$

is

$$1 \to (P_K^{(+)})^G \to I_K^G \to (\mathrm{Cl}\,\theta_K)^G \to H^1(G, P_K^{(+)}) \to 1;$$

if P_k denotes the subgroup of I_K^G consisting of all the fractional ideals that are extended of fractional ideals of $\mathbb{F}_q[T]$, obviously $P_k \subseteq (P_K^{(+)})^G$ and we deduce that

$$1 \to \frac{I_K^G/P_k}{(P_K^{(+)})^G/P_k} \to (\mathrm{Cl}\,\theta_K)^G \to H^1(G, P_K^{(+)}) \to 1 \tag{1}$$

is also exact.

If we look now at the exact sequence

$$1 \to U_K^{(+)} \to K^{(+)} \to P_K^{(+)} \to 1$$

we obtain

$$\begin{aligned} 1 &\to \mathbb{F}_q^* \to k^* \to (P_K^{(+)})^G \to H^1(G, U_K^{(+)}) \to H^1(G, K^{(+)}) \\ &\to H^1(G, P_K^{(+)}) \to H^2(G, U_K^{(+)}) \to H^2(G, K^{(+)}) \to \cdots; \end{aligned} \tag{2}$$

here we have

$$H^2(G, U_K^{(+)}) \simeq \hat{H}^0(G, U_K^{(+)}) = \frac{(U_K^{(+)})^G}{N_{K/k}(U_K^{(+)})} = \frac{\mathbb{F}_q^*}{\mathbb{F}_q^{*l}},$$

$$H^2(G, K^{(+)}) \simeq \hat{H}^0(G, K^{(+)}) = \frac{k^*}{N_{K/k}(K^{(+)})},$$

and the map $H^2(G, U_K^{(+)}) \to H^2(G, K^{(+)})$ may be identified to the canonical map $\mathbb{F}_q^*/\mathbb{F}_q^{*l} \to k^*/N_{K/k}(K^{(+)})$, which is injective because $\mathbb{F}_q^* \cap N_{K/k}(K^{(+)}) = \mathbb{F}_q^{*l}$. Therefore we get from (2) the exact sequence

$$\begin{aligned} 1 \to \frac{(P_K^{(+)})^G}{P_k} &\to H^1(G, U_K^{(+)}) \\ &\to H^1(G, K^{(+)}) \to H^1(G, P_K^{(+)}) \to 1. \end{aligned} \tag{3}$$

In the sequences (1) and (3) all the abelian groups are finite; comparing their orders, it follows at once that

$$\begin{aligned} |(\mathrm{Cl}\,\theta_K)^G| &= \frac{|I_K^G/P_k|\,|H^1(G, P_K^{(+)})|}{|(P_K^{(+)})^G/P_k|} \\ &= \frac{|I_K^G/P_k|\,|H^1(G, K^{(+)})|}{|H^1(G, U_K^{(+)})|}; \end{aligned}$$

applying now Propositions 3.1 and 3.2, and taking into account that $|I_K^G/P_k| = l^s$, which is easily checked, our assertion is proved. ▮

Remark. We can see the analogy between the theorem above and the corresponding result in the classical quadratic number fields setting: in both cases the number of "ambiguous" classes is equal to the degree of the extension Γ/K where Γ is the genus field of K with respect of k. We can note however, that, whereas in the classical context every "ambiguous" class contains an "ambiguous" ideal (that is, an ideal invariant under G), this is not always the case for us, as the following example shows. Let us take $k = \mathbb{F}_q(T)$ with q odd and $K = k(\sqrt{P(T)})$ where $P(T)$ is a monic irreducible polynomial; we have then $|(\mathrm{Cl}\,\theta_K)^G| = 2$. If the degree of $P(T)$ is two and $q \equiv 1 \bmod 4$, it is not difficult to check that the canonical map $I_K^G/P_k \to (\mathrm{Cl}\,\theta_K)^G$ is *not* surjective, hence the class different from the identity in $(\mathrm{Cl}\,\theta_K)^G$ contains no ambiguous ideal.

To conclude this section we shall determine the subgroup of $\mathrm{Cl}\,\theta_K$ which corresponds via the reciprocity isomorphism $\mathrm{Cl}\,\theta_K \simeq \mathrm{Gal}(H^{(+)}/K)$, to the genus field Γ of K. Let τ be a generator of $G = \mathrm{Gal}(K/k)$; we denote

$$(\mathrm{Cl}\,\theta_K)^{\tau-1} = \{[\mathfrak{a}^\tau][\mathfrak{a}^{-1}] \mid [\mathfrak{a}] \in \mathrm{Cl}\,\theta_K\}.$$

PROPOSITION 3.4. *There is a canonical isomorphism*

$$\mathrm{Cl}\,\theta_K/(\mathrm{Cl}\,\theta_K)^{\tau-1} \simeq \mathrm{Gal}(\Gamma/K).$$

Proof. Let us denote $\mathrm{Gal}(H^{(+)}/k) = \mathcal{G}$. The genus field Γ of K is, by definition, the greatest abelian extension of k contained in $H^{(+)}$, that is,

$\Gamma=(H^{(+)})^{\mathscr{G}'}$ is the fixed subfield of $H^{(+)}$ with respect to $\mathscr{G}'$, the derived subgroup of $\mathscr{G}$. To prove our assertion it will suffice to show that the image Ω of $(\mathrm{Cl}\,\theta_K)^{\tau-1}$ via the reciprocity isomorphism $\mathrm{Cl}\,\theta_K \simeq \mathrm{Gal}(H^{(+)}/K)$ coincides with $\mathscr{G}'$.

If $([\mathfrak{a}], H^{(+)}/K) \in \mathrm{Gal}(H^{(+)}/K)$ denotes the Artin symbol of $[\mathfrak{a}]$—for $[\mathfrak{a}] \in \mathrm{Cl}\,\theta_K$—we have

$$\begin{aligned}([\mathfrak{a}]^{\tau-1}, H^{(+)}/K) &= ([\mathfrak{a}]^{\tau}, H^{(+)}/K)([\mathfrak{a}]^{-1}, H^{(+)}/K)\\ &= \bar{\tau}^{-1}([\mathfrak{a}], H^{(+)}/K)\,\bar{\tau}([\mathfrak{a}], H^{(+)}/K)^{-1} \in \mathscr{G}'\end{aligned}$$

(here $\bar{\tau}$ is an arbitrary extension of τ to $H^{(+)}$); it follows that

$$K \subset \Gamma = (H^{(+)})^{\mathscr{G}'} \subset (H^{(+)})^{\Omega} \subset H^{(+)},$$

hence

$$[(H^{(+)})^{\Omega} : K] = (\mathrm{Gal}(H^{(+)}/K) : \Omega) = (\mathrm{Cl}\,\theta_K : (\mathrm{Cl}\,\theta_K)^{\tau-1}).$$

We contend that $(\mathrm{Cl}\,\theta_K : (\mathrm{Cl}\,\theta_K)^{\tau-1}) = l^s$; in fact this is an immediate consequence of the exactness of the sequence

$$1 \longrightarrow (\mathrm{Cl}\,\theta_K)^G \longrightarrow \mathrm{Cl}\,\theta_K \xrightarrow{\tau-1} \mathrm{Cl}\,\theta_K \longrightarrow \frac{\mathrm{Cl}\,\theta_K}{(\mathrm{Cl}\,\theta_K)^{\tau-1}} \longrightarrow 1$$

and Theorem 3.3. Since we have seen in Section 2 that $[\Gamma : K] = l^s$, we have $\Gamma = (H^{(+)})^{\mathscr{G}'} = (H^{(+)})^{\Omega}$; hence $\Omega = \mathscr{G}'$. ∎

4

We now give a characterization of the prime ideals of θ_K which split completely in the genus field Γ of K, similar to the classical result obtained by Hasse [6] in the quadratic number fields context. For that purpose, it is useful to make use of the symbol which describes the behaviour of the prime ideals in Kummer extensions L/k of k, just like the Legendre symbol does for quadratic extensions $F/\mathbb{Q}$; we recall briefly the properties of such a symbol, giving explicitly a reciprocity law (Proposition 4.1 below).

Let $L = k(\sqrt[l]{Q(T)})$ with $Q(T) \in \mathbb{F}_q[T]$, be a Kummer extension of degree l of k, and $\mathfrak{p}$ a prime ideal of $\mathbb{F}_q[T]$, such that $Q(T) \notin \mathfrak{p}$. If $k_{\mathfrak{p}}$ denotes as always the completion of k with respect to the discrete valuation corresponding to $\mathfrak{p}$, and $\hat{\mathfrak{p}}$ the topological closure of $\mathfrak{p}$ in $k_{\mathfrak{p}}$, the local field extension $k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}}$ is unramified, therefore the Frobenius automorphism of $\hat{\mathfrak{p}}$ is characterized by

$$(\hat{\mathfrak{p}}, k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}}) \equiv (\sqrt[l]{Q(T)})^{N\hat{\mathfrak{p}}} \qquad \mathrm{mod}\ \mathfrak{P},$$

where $\mathbb{N}\hat{\mathfrak{p}}$ is the cardinal of the residue field of $\hat{\mathfrak{p}}$ and $\mathfrak{P}$ is the maximal ideal of the valuation ring of $k_{\mathfrak{p}}(\sqrt[l]{Q(T)})$. Since the residue fields of $\hat{\mathfrak{p}}$ and $\mathfrak{p}$ are isomorphic, we have

$$\frac{(\hat{\mathfrak{p}}, k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}})(\sqrt[l]{Q(T)})}{\sqrt[l]{Q(T)}} \equiv (Q(T))^{(\mathbb{N}\mathfrak{p}-1)/l} \qquad \mathrm{mod}\ \mathfrak{P};$$

clearly $\mathbb{N}\mathfrak{p} \equiv 1 \bmod l$, so that both sides of the congruence are in $\mathbb{F}_q[T]$, and hence the congruence is also fulfilled mod $\mathfrak{p}$. Moreover the L.H.S. of the above congruence is an l-root of unity in $\mathbb{F}_q^*$; hence

DEFINITION. For any $Q(T) \in \mathbb{F}_q[T]$ and any prime ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$ such that $Q(T) \notin \mathfrak{p}$, the symbol $(Q(T)/\mathfrak{p})_l \in \mathbb{F}_q^*$ denotes the (unique) l-root of unity such that

$$\left(\frac{Q(T)}{\mathfrak{p}}\right)_l \equiv (Q(T))^{(\mathbb{N}\mathfrak{p}-1)/l} \qquad \mathrm{mod}\ \mathfrak{p}.$$

Therefore we have

$$\frac{(\hat{\mathfrak{p}}, k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}})(\sqrt[l]{Q(T)})}{\sqrt[l]{Q(T)}} = \left(\frac{Q(T)}{\mathfrak{p}}\right)_l;$$

consequently $\mathfrak{p}$ splits completely in the extension $k(\sqrt[l]{Q(T)})/k$ if and only if $(Q(T)/\mathfrak{p})_l = 1$.

This symbol fulfills the obvious properties:

(i) $\forall Q(T),\ R(T) \in \mathbb{F}_q[T],\ Q(T),\ R(T) \notin \mathfrak{p}$, we have

$$\left(\frac{Q(T)}{\mathfrak{p}}\right)_l \left(\frac{R(T)}{\mathfrak{p}}\right)_l = \left(\frac{Q(T)\,R(T)}{\mathfrak{p}}\right)_l,$$

(ii) $\forall Q(T) \in \mathbb{F}_q[T],\ Q(T) \notin \mathfrak{p}$, we have

$$\left(\frac{Q(T)}{\mathfrak{p}}\right)_l = 1 \Leftrightarrow Q(T) + \mathfrak{p} \in (\mathbb{F}_q[T]/\mathfrak{p})^{*l},$$

(iii) $(a/\mathfrak{p})_l = a^{(\mathbb{N}\mathfrak{p}-1)/l},\ \forall a \in \mathbb{F}_q^*$;

besides, it can be extended by multiplicity just as in the case of the classical Jacobi symbol: if $\mathfrak{a}$ is an ideal of $\mathbb{F}_q[T]$ and $Q(T) \in \mathbb{F}_q[T]$ is prime to $\mathfrak{a}$, let $(Q(T)/\mathfrak{a})_l$ be

$$\left(\frac{Q(T)}{\mathfrak{a}}\right)_l = \prod_{\mathfrak{p} \supseteq \mathfrak{a}} \left(\frac{Q(T)}{\mathfrak{p}}\right)_l^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where $v_p(\mathfrak{a})$ is the exponent of $\mathfrak{p}$ in the factorization of $\mathfrak{a}$ as a product of prime ideals.

If $Q(T)$, $R(T) \in \mathbb{F}_q[T]$ are prime to each other, we now obtain explicitly the relation between $(Q(T)/(R(T)))_l$ and $(R(T)/(Q(T)))_l$; like other reciprocity laws, it follows in a natural way from the product formula of class field theory.

For any prime ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$, let us denote, adopting classical notations (see Serre [13, Chap. XIV])

$$(Q(T), R(T))_{\mathfrak{p}} = \frac{(R(T), k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}})(\sqrt[l]{Q(T)})}{\sqrt[l]{Q(T)}},$$

where $(R(T), k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}})$ is the image of $R(T)$ through the local reciprocity map $k_{\mathfrak{p}}^* \to \mathrm{Gal}(k_{\mathfrak{p}}(\sqrt[l]{Q(T)})/k_{\mathfrak{p}})$; the product formula states that $\prod_{\mathfrak{p}} (Q(T), R(T))_{\mathfrak{p}} = 1$, where $\mathfrak{p}$ runs over all prime divisors of k.

PROPOSITION 4.1. *Let $Q(T)$, $R(T) \in \mathbb{F}_q[T]$ be irreducible non-associated polynomials, and $\delta(Q)$, $\delta(R)$ be their respective degrees. If a_0, b_0 are their respective leading coefficients, the following formula holds*

$$\left(\frac{R(T)}{(Q(T))}\right)_l^{-1} \left(\frac{Q(T)}{(R(T))}\right)_l \left[\frac{(-1)^{\delta(Q)\delta(R)} b_0^{\delta(Q)}}{a_0^{\delta(R)}}\right]^{(q-1)/l} = 1.$$

Proof. Since $k_\infty(\sqrt[l]{Q(T)})/k_\infty$ is a Kummer tamely ramified (or unramified) extension of local fields, its reciprocity map is well known (see Serre [13, Chap. XIV, Prop. 8]), and we have

$$(Q, R)_\infty \equiv \left(\frac{(-1)^{\delta(Q)\,\delta(R)} R^{\delta(Q)}}{Q^{\delta(R)}}\right)^{(q-1)/l} \qquad \mathrm{mod}\ \infty;$$

but

$$\frac{R^{\delta(Q)}}{Q^{\delta(R)}} \equiv \frac{b_0^{\delta(Q)}}{a_0^{\delta(R)}} \qquad \mathrm{mod}\ \infty,$$

hence

$$(Q, R)_\infty = \left[\frac{(-1)^{\delta(Q)\,\delta(R)} b_0^{\delta(Q)}}{a_0^{\delta(R)}}\right]^{(q-1)/l}.$$

On the other hand, for any prime ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$ such that $v_{\mathfrak{p}}(Q) = 0$ and $v_{\mathfrak{p}}(R) = 1$, we have

$$(Q, R)_{\mathfrak{p}} = \left(\frac{Q}{(R)}\right)_l;$$

if $v_{\mathfrak{p}}(Q)=1$ and $v_{\mathfrak{p}}(R)=0$,

$$(Q, R)_{\mathfrak{p}}=(R, Q)_{\mathfrak{p}}^{-1}=\left(\frac{R}{(Q)}\right)_l^{-1}.$$

Now the proposition follows directly from the product formula. ∎

Remarks. (1) If Q and R are monic the above theorem gives

$$\left(\frac{R}{(Q)}\right)_l^{-1}\left(\frac{Q}{(R)}\right)_l=(-1)^{\delta(Q)\,\delta(R)(q-1)/l}.$$

(2) Proposition 4.1 may be generalized to polynomials $Q, R\in\mathbb{F}_q[T]$ prime to each other but not necessarily irreducible.

Before giving a description of the prime ideals of θ_K which split completely in the genus field Γ, let us make a simple remark. If for any monic irreducible divisor $P_i(T)$ of $P(T)$, we denote by $P_i^*(T)$ the polynomial $(-1)^{d_i}P_i(T)$ where $d_i=\deg(P_i(T))$, we have

$$\Gamma=\mathbb{F}_{q^l}(T, \sqrt[l]{P_1^*(T)}, ..., \sqrt[l]{P_s^*(T)})$$

(this is clear since $q\equiv 1 \bmod l$ yields $\sqrt[l]{-1}\in\mathbb{F}_{q^l}$).

THEOREM 4.2. *A necessary and sufficient condition for a prime ideal* $\mathfrak{p}$ *of* θ_K *to split completely in the genus field* Γ *of* K, *is that for* $i=1, ..., s$ *the prime ideal* $(P_i(T))$ *of* $\mathbb{F}_q[T]$ *splits completely in the extension* $k(\sqrt[l]{g(T)})/k$*—where* $g(T)$ *is the monic generator of* $N\mathfrak{p}$, *ideal norm of* $\mathfrak{p}$ *with respect to the extension* K/k*—and that* l *divides the absolute degree of* $\mathfrak{p}$ (*which coincides with* $\deg g(T)$).

Proof. We have

$$\begin{aligned}\mathfrak{p}\text{ splits completely in }\Gamma/K &\Leftrightarrow (\mathfrak{p}, \Gamma/K)=1\\ &\Leftrightarrow (\mathfrak{p}, \Gamma/K)|_{K(\sqrt[l]{P_i^*(T)})}=1 \quad \forall i=1, ..., s \text{ and } (\mathfrak{p}, \Gamma/K)|_{\mathbb{F}_{q^l}(T)}=1\\ &\Leftrightarrow (N\mathfrak{p}, k(\sqrt[l]{P_i^*(T)})/k)=1 \quad \forall i=1, ..., s \text{ and } (N\mathfrak{p}, \mathbb{F}_{q^l}(T)/k)=1\\ &\Leftrightarrow \left(\frac{P_i^*(T)}{N\mathfrak{p}}\right)_l=1 \quad \forall i=1, ..., s \text{ and } \left(\frac{\xi}{N\mathfrak{p}}\right)_l=1,\end{aligned}$$

where ξ is a generator of $\mathbb{F}_q^*$.

If m is the degree of $g(T)$, so that the cardinal of $\theta_K/\mathfrak{p}$ is $\mathbb{N}\mathfrak{p}=q^m$, by the reciprocity law proved above we have

$$\left(\frac{P_i^*(T)}{N\mathfrak{p}}\right)_l=\left(\frac{-1}{N\mathfrak{p}}\right)_l^{d_i}\left(\frac{P_i(T)}{N\mathfrak{p}}\right)_l=(-1)^{((\mathbb{N}\mathfrak{p}-1)/l)d_i}\left(\frac{P_i(T)}{N\mathfrak{p}}\right)_l$$

$$=(-1)^{((\mathbb{N}\mathfrak{p}-1)/l)d_i}(-1)^{md_i(q-1)/l}\left(\frac{g(T)}{(P_i(T))}\right)_l$$

$$=\left(\frac{g(T)}{(P_i(T))}\right)_l;$$

the last equality holds obviously if q is even, that is, K of characteristic 2; if q is odd, the exponent of -1 is

$$\frac{q^m-1}{l}d_i+md_i\frac{q-1}{l}=d_i\frac{q-1}{l}[(1+q+\cdots+q^{m-1})+m]$$

$$\equiv d_i\frac{q-1}{l}(m+m)\equiv 0 \qquad \text{mod } 2.$$

That is, $\mathfrak{p}$ splits completely in Γ iff

$$(P_i(T),k(\sqrt[l]{g(T)})/k)=1 \qquad \forall i=1,\ldots,s \text{ and } \xi^{(\mathbb{N}\mathfrak{p}-1)/l}=1;$$

since the last condition holds iff $l\mid m$, the theorem is proved. ∎

Acknowledgment

I am indebted to Dr. J. M. Souto for his suggestions, valuable comments, and constant support.

References

1. E. Artin and J. Tate, "Class Field Theory," Benjamin, New York/Amsterdam, 1967.
2. J. W. S. Cassels and A. Fröhlich (Ed.), "Algebraic Number Theory," Proceedings of a Conference organized by the L.M.S., Academic Press, London, 1967.
3. C. Chevalley, "Introduction to the Theory of Algebraic Functions of One Variable," A.M.S. Surveys, 1951.
4. Y. Furuta, The genus field and genus number in algebraic number fields, *Nagoya Math. J.* **29** (1967), 281–285.
5. L. Goldstein, On prime discriminants, *Nagoya Math. J.* **45** (1971), 119–127.
6. H. Hasse, Zur Geschlechtertheorie in quadratischen Zahlkorpern, *J. Math. Soc. Japan* **3** (1951), 45–51.

7. D. R. HAYES, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974). 77–91.
8. D. R. HAYES, Explicit class field theory in global function fields, *in* "Studies in Algebra and Number Theory," pp. 173–217, Academic Press, New York, 1979.
9. M. ISHIDA, The genus fields of algebraic number fields, *in* "Lecture Notes in Math.," Vol. 555, Springer-Verlag, Berlin, 1976.
10. M. ROSEN, *S*-units and *S*-class groups in algebraic function fields, *J. Algebra* **26** (1973), 98–108.
11. M. ROSEN, Ambiguous divisor classes in function fields, *J. Number Theory* **9** (1977), 160–174.
12. M. ROSEN, The Hilbert class field in function fields, *Exposition. Math.* **5** (1987), 367–378.
13. J. P. SERRE, "Corps Locaux," Hermann, Paris, 1968.